



INFRASTRUCTURE SERVICES AND SUPPORT CONTRACT

CURRENT ITID INFRASTRUCTURE SERVICES

June 4, 2001

TABLE OF CONTENTS

1	CUSTOMER SUPPORT CENTER	5
1.1	CSC Help Desk Operations	5
1.1.1	CSC Service Request Preparation	5
1.1.2	CSC Service Request - Problem Requests	6
1.1.3	CSC Service Request - End-user Questions	6
1.2	SWAT Requests	7
1.3	Special Handling	7
1.4	Knowledge Bases	7
1.5	Web Enabled Services	7
1.6	Reporting	7
2	DESKTOP SERVICES	8
2.1	Maintenance	8
2.1.1	Hardware Maintenance	8
2.1.2	Spare Parts	9
2.1.3	Special Maintenance	9
2.1.4	Software Maintenance	9
2.1.5	Diagnostic Utilities	9
2.1.6	Warranties	9
2.1.7	Reporting	10
2.2	Installation/Deployment	10
2.2.1	CSC Service Requests	10
2.2.2	Network Coordination	10
2.2.3	Hardware Coordination	10
2.2.4	Software Coordination	11
2.3	ADAMS Support	11
2.4	Non-Infrastructure Acquisitions	12
2.5	Procurement	12
2.5.1	Hardware/Software	12
2.5.2	Spare Parts	12
3	NETWORK SERVICES	13
3.1	Network Operations Center (NOC)	13
3.2	Current NOC Operations	14
3.2.1	Network Management	14
3.2.2	CSC Service Requests	15
3.2.3	Failures	15
3.2.4	Service Provisioning	16
3.2.4.1	Remote Access System	16
3.2.4.2	Resident Inspector Sites Frame Relay Connections	16
3.2.4.3	WAN Connectivity	16
3.2.5	On-call Operations	16
3.3	Maintenance	16
3.3.1	Hardware Maintenance	16
3.3.2	Spare Parts	17
3.3.3	Software Maintenance	17
3.3.4	Special Maintenance	17

3.3.5	Reporting	17
3.4	Installation/Deployment	18
3.4.1	New Systems	18
3.4.2	Relocations	18
3.5	Procurement	18
3.6	Regional LAN Administrator Support	18
4	INFRASTRUCTURE DEVELOPMENT AND IMPLEMENTATION SERVICES	22
4.1	Systems Engineering	22
4.1.1	IT Infrastructure Development	22
4.1.2	IT Infrastructure Integration	22
4.1.3	IT Infrastructure Implementation	22
4.2	IT Infrastructure Services	23
4.2.1	Workstation System Services	23
4.2.2	Local and Wide Area System Services	23
4.2.2.1	Infrastructure Services	23
4.2.2.2	Web Architecture Services	23
4.2.2.3	LAN/WAN Server Services	23
4.2.3	High Performance Computing Environment (HPCE) Services	23
4.2.4	Other IT Infrastructure Services	24
4.2.4.1	IT Infrastructure Security Services	24
4.2.4.2	Contingency Management	24
4.2.4.3	Procurement	24
4.3	Development, Integration, and Implementation Life-Cycle	25
4.3.1	Detailed Requirements Analysis	25
4.3.2	Design	25
4.3.3	New Technology Development	26
4.3.4	New Technology Acceptance Testing	26
4.3.5	Transition to Production Operational Support	26
4.3.6	Implementation	27
4.3.7	Position Descriptions	27
5	PROGRAM SERVICES	35
5.1	Quality Management	35
5.1.1	Program Management	35
5.1.2	Metrics and Performance Criteria	35
5.1.3	End-User Satisfaction Monitoring	35
5.1.4	Trend Analysis	35
5.1.7	Audits	36
5.2	Configuration Management	36
5.2.1	Program Management	36
5.2.2	Change Management	36
5.2.3	Hardware/Software Inventory	36
5.2.4	Configuration Management Data Base (CMDB)	37
5.2.5	Configuration Reporting	37
5.3	Contingency Management	37
5.3.1	Program Management	37
5.3.2	Backup	37
5.3.3	Disaster Recovery	37
5.4	Documentation Management	38

5.4.1	Program Management	38
5.4.2	Procedures	38
5.5	Security Management	38
5.5.1	Program Management	38
5.5.2	System	38
5.5.3	Network/Cyber	39
5.5.4	Physical	39
5.5.5	Audits	39
5.6	Independent Audit and Verification	40
6	RELATED NRC IT SERVICES	41
6.1	TELECOMMUNICATIONS SERVICES	41
6.2	DATA CENTER SERVICES	41
6.3	EMERGENCY OPERATIONS CENTER	42

CURRENT ITID INFRASTRUCTURE SERVICES

1 CUSTOMER SUPPORT CENTER

The Customer Support Center (CSC) Help Desk provides single point of contact for primary immediate IT support and assistance to NRC end-users. The CSC is responsible for providing a single common telephone number for assisting the NRC HQ staff in the proper use and maintenance of the NRC IT infrastructure systems and applications used to accomplish the mission and program activities of the NRC. The CSC provides first-line problem diagnosis and resolution for desktops, networks, telephones, Agencywide applications, Agency-developed applications, minicomputers, mainframe computers, and timesharing services.

The CSC provides Tier 1 (telephone) support, which includes problem resolution, reporting, assigning, tracking, and escalation services for NRC end-user reported questions, problems, and requests for new or changed services related to IT Infrastructure systems and applications. The CSC responds by telephone to end-user requests for common operational problems and questions. The CSC is responsible for resolving operational problems using remote diagnostic and correction facilities whenever possible. If required, CSC Tier 1 support includes CSC assignment of the initial action to the appropriate support group, however CSC maintains responsibility for processing, prioritizing, escalating, and tracking CSC Service Requests to closure.

The Regions currently provide Help Desk services, installation, warranty and out-of-warranty maintenance to their Regional offices and their Resident Inspector sites.

1.1 CSC Help Desk Operations

The CSC Help Desk provides support for NRC Headquarters user questions and service requests, coordinates support activities with other support components, and confirms customer satisfaction with the service provided.

This group is responsible for assignment of the initial action to the appropriate group and follow-thru to closure of the CSC Service Request.

- Provide problem resolution, reporting, assigning, tracking, and escalation services for NRC end-user reported questions and problems related to desktop systems hardware and software, the NRC network, NRC Telecom services, Data Center, and timesharing services.
- Answer all telephone calls to the CSC
- Respond by telephone to requests from: Email, memos, voice-mail, NRC forms, the OCIO desktop support group, or the Network Operations Center in accordance with service level requirements.
- Resolve the customers request on the first phone call whenever possible

1.1.1 CSC Service Request Preparation

- The CSC utilizes the McAfee automated system to track and report on Service Requests.
- Create a CSC Service Request utilizing the CSC Service Request Tracking System for each end-user reported problem or question.

- Notify customers of the CSC Request Number assigned to a Service Request.
- Establish the problem severity level on each CSC Service Request.
- Change priority on open CSC Service Requests as needed.
- Maintain ownership of CSC Service Requests and monitor progress until problem resolution.
- Contact the end-user to provide CSC Service Request status updates and anticipated problem resolution.
- Confirm that problems are resolved to customer satisfaction.
- Close CSC Service Requests upon customer confirmation of resolution.

1.1.2 CSC Service Request - Problem Requests

- Create a CSC Service Request for every end-user reported problem.
- Resolve end-user problem over the telephone or remotely whenever possible.
- Provide knowledge base, troubleshooting and diagnostic support to identify and resolve end-user problems.
- Resolve problems related to desktop systems such as incorrect set-up, customization, incorrect use of the system, and user changes to standard configurations, etc.
- Resolve routine network-related items such as LAN printer problems, password resets, LAN disk space allocations, and workstation Network software.
- Analyze, diagnose, and resolve problems from a total NRC systems perspective.
- Respond to recurring problems.

1.1.3 CSC Service Request - End-user Questions

- Create a CSC Service Request for every end-user question.
- Respond to end-use questions related to:
 - The procurement of IT resources.
 - The utilization of supported hardware and software.
 - The utilization of supported commercial off-the-shelf (COTS) software.
 - The utilization of all Agency wide systems.
 - The utilization of NRC developed applications.
 - Requests for general information.

1.2 SWAT Requests

- Coordinate SWAT (scheduled work activities) requests among the OCIO support groups to assure resolution of problems that cannot be resolved over the telephone, by on-site support, or by consulting services.

1.3 Special Handling

- Respond to requests for special handling, escalation, or higher priority on specifically identified requests.
- Escalate requests to a higher level of support in accordance with NRC policies, procedures and service level requirements.

1.4 Knowledge Bases

- Maintain an automated knowledge base of information to facilitate user support and end-user self-help.
- Maintain the knowledge base and keep it updated with current information as problem resolutions become known.
- Utilize the knowledge base whenever applicable.

1.5 Web Enabled Services

- Maintain a web-accessible database to allow users to monitor CSC Service Request status.
- Maintain on a monthly basis, a web-accessible database of end-user frequently asked questions (FAQ).

1.6 Reporting

- Prepare briefings and attend the daily CSC operational status meeting as requested.
- Prepare briefings and attend the weekly operational status meeting as requested.
- Prepare the summary report for the monthly CSC performance report.

2 DESKTOP SERVICES

Desktop Services provide all NRC personnel with a standard desktop workstation that is an Intel-based processor using the Microsoft NT Workstation operating system. Desktop Services also provides installation and all Tier 2 (on-site) maintenance and upgrade services to HQ Offices. Desktop installation and maintenance and Tier 2 support in the Regions is supplied by the Regions.

Headquarters Desktop Services is broken into three areas:

PC Refresh. Replacement of the desktop (or equivalent) business application microcomputer inventory for the entire Agency.

During 1997-1999, most of NRC PC's were upgraded for Y2K compliance. The current NRC budget allocates funds for a 15% refresh rate. Funds available at the end of each fiscal year are also sometimes allocated to equipment refresh if an upgrade requirement is identified that supports new NRC application requirements

The current specifications for NRC's personal computers are:

Hardware:

Standard PC: 500Mz, 8.4 GB HD, 128 DIMM SDRAM, 19" monitor.

Software:

Core: Corel WordPerfect Suite 8.0, Windows NT 4.0, GROUPWISE 5.0, Novell NetWare Suite, Norton Virus Control, Netscape, CITRIX Web-based Applications, Agency Documents Access and Management System (ADAMS)

Additional: Microsoft Word, Excel and PowerPoint.

Desktop Services. Maintenance of the business applications microcomputer inventory for the Headquarters Office. This includes maintaining basic desktop workstations and peripheral equipment that support NRC staff at their primary work locations, and includes the high performance workstations.

Desktop systems support functions for the Headquarters Office include installations of new software and hardware, system relocations, routine maintenance, back-ups, data and system restorations, documentation, security, and technical services.

Non-Infrastructure Acquisitions. Acquisition and installation of special purpose workstation hardware and software for the Headquarters Office. Provide for acquisition and installation of non-infrastructure workstation hardware and software requested and funded by offices, including such items as engineering workstations, portable computers, scanners, tape drives, printers, non-standard monitors, memory, CD-ROMs, special software, and larger hard drives.

2.1 Maintenance

2.1.1 Hardware Maintenance

- Perform Tier 2 troubleshooting and diagnostics to ensure that all supported hardware is performing in accordance with service level requirements.
- Identify failing hardware and restore to service in accordance with service level requirements.
- Install upgrades, modifications, and maintenance releases in accordance with service level requirements, including engineering changes, maintenance updates, and upgrades.
- Perform preventive maintenance in accordance with service level requirements, including engineering changes, maintenance updates, and upgrades.
- Maintain service/repair logs for each supported hardware system and its components.

2.1.2 Spare Parts

- Provide an on-site stock of spare parts and components needed for the repair of all maintained hardware.

2.1.3 Special Maintenance

- Provide special maintenance as requested.

1.4 Software Maintenance

- Perform Tier 2 troubleshooting and diagnostics to ensure that supported software is performing in accordance with service level requirements.
- Identify failing software and restore to service in accordance with service level requirements.
- Install maintenance releases in accordance with service level requirements, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance in accordance with service level requirements, including engineering changes, maintenance updates, patches, and upgrades.

2.1.5 Diagnostic Utilities

- Perform hardware and software diagnostics as appropriate to maintain service levels.

2.1.6 Warranties

- Ensure compliance with supported hardware and software license and warranty restrictions.

- Register hardware and software as necessary with vendors in order to receive notices and maintenance updates.
- Keep and maintain warranty service and repair logs for each hardware and software license.
- Track warranties to ensure compliance.
- Adhere to and enforce vendor warranty contracts and agreements.

2.1.7 Reporting

- Summarize all system down times and problems and current status in the weekly report and attach a copy of the system trouble logs.

2.2 Installation/Deployment

2.2.1 CSC Service Requests

- Install new desktop system components, relocate desktop components, install upgrades, modifications, and peripherals in response to approved CSC Service Requests.
 - Provide integrated, working, and tested systems with configurations that comply with NRC standards and specifications.
 - Schedule installations i
 - Perform pre-install walk-through to prevent move-related problems.
 - Deliver, set-up, and test installations.
 - Establish system and application functionality and connectivity after installation.
 - Installation is complete when all applications, including those requiring network access, are installed and working to the satisfaction of the user.
 - Deinstall, remove and dispose of surplus, failing, or obsolete hardware and software according to NRC procedures, as requested

2.2.2 Network Coordination

- Coordinate with the network support vendors prior to system installation to ensure that the network software and hardware is properly configured to support and recognize the new system, using established coordination and communication procedures.

2.2.3 Hardware Coordination

- Ensure that the electrical power and network connections are working.
- Coordinate with the facilities, electrical, and cabling vendors prior to delivery, to ensure that the site is prepared.
- Provide furniture or cabinets as required, with NRC approval.

2.2.4 Software Coordination

- Ensure that original system software image and customer data is preserved (backed up) prior to commencing work so that the system can be restored to its original state if necessary.
- Perform minor customization and integration modifications of the systems as necessary to maintain continued operations after installation.
- Ensure that modifications are in compliance with NRC configuration standards.

2.3 ADAMS Support

The NRC Agencywide Documentation And Management System (ADAMS) is a significant initiative currently underway at NRC. ADAMS is an electronic document and records management system that maintains NRC's unclassified official program and administrative records in a centralized electronic document repository. The major components of ADAMS include FileNet's Integrated Document Management software and other related applications that are integrated and operate in Windows NT, Novell, and GroupWise environments.

For ADAMS, ITID provides the following Operations and Maintenance support:

- Maintain ADAMS document entry workstations
- Maintain ADAMS servers
- Develop and run reports on ADAMS system use, performance and availability
- Provide ADAMS Training Services through the CSC

Other OCIO organizations provide user training and assistance in performing the following document management tasks: data entry; document entry; indexing documents; setting access privileges for documents; retrieving documents; printing of documents; electronic distribution of documents; electronic signatures on documents; archiving documents; and document scanning functions

- Provide Tier 2 customer support for ADAMS software and equipment including.
 - Document entry
 - Indexing
 - Security
 - Retrieval
 - Printing
 - Distribution
 - Electronic signatures
 - Archiving

- Document Management
- Provide Tier 2 ADAMS Administration support including:
 - Develop and run reports
 - Troubleshoot problems
 - Define and maintain user and group profiles
 - Manage searches
 - Provide support for logins/passwords
 - Monitor system logs
 - Assist in the reclaim process
 - Assist in establishing and maintaining:
 - User naming conventions
 - Libraries
 - Folders
- Develop and maintain work flow in a Novell GroupWise, Microsoft NT, and ADAMS/FileNET environment.
- Provide on the job training to others as needed.
- Create/update records in NRC's tracking system and in other systems.
- Participate in information gathering, technical problem studies, and evaluation of software and hardware as needed.
- Become knowledgeable of and perform work within the guidelines of established NRC policies and procedures pertaining to ADAMS.

2.4 Non-Infrastructure Acquisitions

- Provide for acquisition and installation of non-infrastructure workstation hardware and software requested and funded by offices, including such items as engineering workstations, portable computers, scanners, tape drives, printers, non-standard monitors, memory, CD-ROMs, special software, and larger hard drives.

2.5 Procurement

2.5.1 Hardware/Software

- Order hardware and software accordance with service level requirements.
- Order hardware and software maintenance releases, including engineering changes, maintenance updates, fixes, and upgrades.
- Arrange for maintenance agreements and support from hardware and software providers as appropriate.

- Purchase hardware and software diagnostic utilities as appropriate to maintain service levels.

2.5.2 Spare Parts

- Purchase and spare desktop system parts and components needed to assure continued operation of supported hardware.

3 NETWORK SERVICES

The current NRC IT Infrastructure Architecture provides an Agencywide standard method for delivering IT services to the desktops of NRC employees and designated Contractors; and facilitating communications with external organizations such as other domestic and foreign government agencies, nuclear power plants, laboratories and the general public.

Network Services administration and operational support functions include installation, troubleshooting, diagnostics, operation, maintenance, management, and administration of the NRC data, voice, and video communications infrastructure. Network services provide NRC users with shared network storage, network printers, E-Mail, Internet and Intranet browsing services, remote applications connectivity, and nationwide access to Agencywide applications.

The Network Services *Information Technology Architecture* Report dated September 13, 1999, and an NRC network equipment inventory list, *List of Equipment*, is provided in Section J to provide further details on the NRC Network.

3.1 Network Operations Center (NOC)

The NRC Network Operations Center (NOC) operates and maintains services Agencywide to monitor network operations, track network performance, and troubleshoot problems to restore degraded network hardware, and applications software elements to service. The NOC is also responsible for scheduling, coordinating and implementing all upgrades to equipment and software associated with network services. The NOC uses state of the art network tools such as Optivity and Openview are used to monitor and maintain the infrastructure, E-mail services, IP services and application services.

Network component systems include: hubs, routers, communication links, Regional links, and all other supporting data communications for NRC's Network operations. Also included are systems that primarily support the Network infrastructure, including: network servers, file servers, message (E-Mail) servers, gateway servers, web servers, bastion hosts, and firewall systems.

HQ workstations are connected to an Ethernet local area network (LAN). Each NRC location uses the same architecture for its LAN installations. The Agency's computer centers, including its servers and mini-computers, are connected to the NRC Headquarters backbone network via . External networks, Internet services, and timesharing services are also connected to the NRC backbone network utilizing cyber security systems such as firewalls.

- Identify, evaluate, develop and implement network management processes and procedures from an operational support perspective to perform proactive fault management, performance management, growth management, and security management for all network components, systems, and services
- Implement and operate network services performance measurement systems to provide periodic reports to NRC management on network services performance relative to the NRC customer service level requirements and service level agreements.
- Plan and manage network growth by predicting future trends based on historical network trends and business information

3.2 Current NOC Operations

- Operate the network during designated hours and monitor availability and performance.
- Operate the network to provide consistent operation and optimum performance.
- Provide the NOC Monthly Security Report
- Provide operational support for E-mail and Internet server applications administration, systems programming support, database administration, hardware/software configuration, and inter-system communications.
- Perform integration testing and approve new Desktop PC hardware, software, and peripheral systems for installation into the network infrastructure Production Operations Environment (POE).
- Procure, integrate, test, and coordinate installation of network-related hardware and software on Desktop PC systems, such as NetWare and Citrix clients, network interface cards, network printer drivers, etc.
- Provide and maintain an automated software distribution system for the software installed on Desktop PC's and network servers.
- Provide network availability and response according to NRC service level requirements.
- Perform diagnosis, identification, and correction of failing network components or failure of the interfaces between network components and other systems, operating environments, or applications.
- Use tools to remotely identify and diagnose network problems.
- Monitor availability and status of network systems.

3.2.1 Network Management

- Identify, evaluate, develop and implement network management from an operational support perspective to perform proactive fault management, performance management, growth management, security management, asset management, for all network components, systems, and services.
- Identify and implement metrics and thresholds to measure and manage fault, growth, performance, security, and accounting for the network using automated network tools.
- Measure performance of network components for compliance with manufacturer's published performance specifications for network hardware and software.
- Gather and analyze network and desktop statistical information and provide recommendations to improve network performance.
- Identify and resolve problems proactively before they affect users in order to ensure high network availability and reliability.

- Consolidate network tools into an integrated network management system.
- Maintain and operate network tools which are available for the routine operation and maintenance and monitoring of network components, services and systems.
- Provide operational support for network tools during the development of new technology to ensure maintainability and supportability of new technology.
- Review the current network tools and make recommendations for their enhancements or replacement.
- Develop and implement new capabilities to perform the required network management functions based on the implementation of new technology.
- Plan and manage network growth by predicting future trends based on historical network trends and business information.
- Monitor and manage network traffic patterns and identify issues such as "bottlenecks" that may reduce performance.
- Provide routine reports on system status and availability of network components, systems, and services.
- Monitor and manage in realtime the availability of network components, systems, and services for optimum performance and availability.

3.2.2 CSC Service Requests

- Work closely with and support the Help Desk Contractor in resolving user problems related to the network infrastructure, LAN logon and User ID administration, file security, and security services, including network failures or failures of network interfaces to other systems.
- Work closely with and support the Desktop PC maintenance Contractors in resolution of Desktop PC software and hardware problems. Respond to requests for assistance from the Desktop PC maintenance Contractors. Support Desktop PC refresh activities.
- Work closely with and support the Cable Plant and Telecommunications Contractors in resolving user problems related to network infrastructure systems or requiring diagnostics from network infrastructure management systems.
- Dispatch appropriate maintenance personnel to resolve the CSC Service Request.
- Record observations and conclusions on CSC Service Requests.
- Monitor progress until problem is resolved.
- Provide CSC periodic status reports on CSC Service Requests and respond to status inquiries from CSC.

3.2.3 Failures

- Identify and resolve problems proactively before they affect users in order to ensure high network availability and reliability
- Respond to all reports of network failures or failures of network interfaces to other systems.
- In the event of a failure, take immediate corrective actions to restore the network to service.
- In the event of a failure notify the CSC of the expected time to repair and return the network to service.

3.2.4 Service Provisioning

3.2.4.1 Remote Access System

- Perform order entry activities for Remote Access System dial-up phone lines from the appropriate telecommunications service provider for headquarters and regional offices as required.
- Place requests for moves, additions and changes to existing remote access dial-up phone lines.
- Confirm receipt of new services, service changes or disconnect orders for remote access dial-up phone lines.

3.2.4.2 Resident Inspector Sites Frame Relay Connections

- Perform order entry activities for frame relay connectivity from the appropriate telecommunications service provider for headquarters, regional offices and resident inspector sites as required.
- Place requests for moves, additions and changes to existing frame relay services and connections.
- Confirm receipt of new services, service changes or disconnect orders for frame relay connections.

3.2.4.3 WAN Connectivity

- Perform order entry activities for WAN connectivity from the appropriate telecommunications service provider for headquarters, regional offices and resident inspector sites as required.
- Place requests for moves, additions and changes to existing WAN services and connections.
- Confirm receipt of new services, service changes or disconnect orders for WAN connections.

3.2.5 On-call Operations

- Provide support for extenuating events outside normal operational periods as required to maintain network systems.

3.3 Maintenance

3.3.1 Hardware Maintenance

- Perform required maintenance on all network hardware.
- Install upgrades, modifications, service releases, and maintenance releases for network hardware, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance on network hardware, including engineering changes, maintenance updates, patches, and upgrades.
- Maintain network hardware service and repair logs for all network systems which will record system down times, problems, causes, resolution, and status.

3.3.2 Spare Parts

- Provide an on-site stock of spare parts and components needed for the repair of all network hardware.

3.3.3 Software Maintenance

- Provide maintenance of all supported network software.
- Install upgrades, modifications, service release, and maintenance releases to network software as necessary to meet the service levels and refresh intervals, including engineering changes, maintenance updates, patches, and upgrades.
- Perform preventive maintenance on network software as necessary to meet the service levels and refresh intervals, including engineering changes, maintenance updates, patches, and upgrades.

3.3.3.1 Warranties

- Ensure compliance with network hardware and software license and warranty restrictions.
- Register network hardware and software as necessary with vendors in order to receive notices and maintenance updates.
- Keep and maintain warranty period, service, and repair records for each network hardware and software license.
- Adhere to and enforce vendor contracts warranties and agreements on network hardware and software.

3.3.4 Special Maintenance

- Provide special maintenance as requested.
- Respond to special maintenance requirements at Regional and other NRC offices.

3.3.5 Reporting

- Summarize network hardware service and repair logs including current status in the weekly report and attach a copy of the system trouble logs.
- Notify NRC immediately when any system goes down or is malfunctioning.
- Provide reports on the performance and availability of LAN and WAN cable, telecommunications, and desktop systems.

3.4 Installation/Deployment

3.4.1 New Systems

- Provide configuration, integration, installation and operational support and administration for network components, network connectivity, and software distribution for new agency systems, services, and business applications.
- Validate system functionality and connectivity after installation; following NRC policies and procedures for installations.

3.4.2 Relocations

- Relocate network systems in accordance with validated move requests.
- Schedule network moves in accordance with NRC policies, procedures and service level requirements.
- Re-establish system functionality and connectivity after moves, following NRC policies and procedures for installations.

3.5 Procurement

3.5.1 Hardware/Software

- Order hardware and software maintenance releases in accordance with NRC policies, procedures and service level requirements, including engineering changes, maintenance updates, fixes, and upgrades.
- Arrange for maintenance agreements and support from hardware and software providers as appropriate.
- Purchase hardware and software diagnostic utilities as appropriate.

3.5.2 Spare Parts

- Purchase and stock spare desktop system parts and components as needed.

J.6 Regional LAN Administrator Support

- Provide first and second level Regional LAN Administrator Support to maintain and support the network including:
 - Hardware
 - Software application problems
 - Analyzing and resolving from a total systems perspective desktop, software and networking problems including:
 - Providing password resets
 - LAN disk space allotment
 - Network printer configuration
 - Operating, monitoring, and administering network components, associated peripheral equipment, and the overall network environment
 - Performing daily backups of file servers and applications servers
 - Identifying, troubleshooting, answering questions, and resolving problems for COTS software applications.

POSITION DESCRIPTION

Position: COOP LAN Administrator

Functions: Monitor, install, integrate, operate, maintain, and support the servers, workstations and printers, associated peripheral equipment, and network environment. Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Recognizes problems and requests assistance. Communicates effectively with end-users, technical support staff and management. Provides status reports regarding operational problems, issues, failures, and outages. Update and maintain operational system documentation and standard operating procedures.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Three (3) years experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN and LAN/WAN operations is desired. This position requires a sound knowledge of local area networks, network security, routing protocols, and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

POSITION DESCRIPTION

Position: Regional LAN Administrator

Functions: Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Operates, monitors, installs, and administers servers, workstations and printers, associated peripheral equipment, and network environment. Recognizes problems and requests assistance. Communicates effectively with end-users, technical support staff and management.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Three (3) year experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN operations is desired. This position requires a sound knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

POSITION DESCRIPTION

Position: ADAMS System Administrator

Functions: Provide client support and systems administration for ADAMS, including software installation, configuration, administration, and support for Saros, Ensemble, Panagon/Mezzaine, @Mezzaine, Watermark, IQ-Objects/Report Manager, Foremost, and other related software (e.g., Internet software, etc.) at the desktop and scanning stations. Perform some server level processes (e.g. Fileshare functions). Provide support for document entry, indexing, retrieval, printing, distribution, archiving, management, and scanning (including Watermark Workstation Administration). Develop and run reports; test and evaluate software; troubleshoot problems; define and maintain user and group profiles; manage searches; provide support for logins/passwords; assist in the reclaim process; assist in establishing and maintaining user naming conventions and folders; and develop and maintain work flow in a Novell GroupWise, Microsoft NT, and FileNET environment.

The specific software packages and versions used may change over time.

Create and maintain local operating and quality assurance procedures and develop recommendations for revising business processes where possible. Provide client support services and procedural assistance to users and assist in the development of training materials. Provide on the job training to others as needed. Process scanning requests and security authorization forms, and carry out other activities. Participate in information gathering, technical problem studies, and evaluation of software and hardware as needed.

Skills:

- Strong analytical skills
- Good organization skills

- Ability to provide first level support in a courteous and professional manner
- Ability to effectively communicate verbally and in writing
- Ability to work independently or as a team leader or member as required
- Ability to install and configure software
- Ability to perform system administration functions

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement. Certification or completion of substantial training in a related personal computer, network, or imaging field may be substituted for part or all of the above requirement.

Experience:

A minimum of five (5) years system configuration, administration, or support experience in an automated imaging or other complex computing environment such as Microsoft NT or Novell environment is required for this position. Three years must be specialized experience as a Novell or NT LAN Administrator. The remainder may be specialized or general experience.

This position requires three years of FileNET administration or support experience, or the satisfactory completion of FileNET training.

POSITION DESCRIPTION

Position: High Performance Computing LAN Administrator

Functions: Operate, monitor, and administer high performance workstations, servers and associated peripheral equipment, and network environment. Integrate and ensure operability of applications and scientific codes into the high performance computing environment. Provides user specific support such as troubleshooting and solving software problems, and determining hardware problems. Communicates effectively with end-users, technical support staff and management. Coordinates high performance computing equipment maintenance. Provides status reports regarding operational problems, issues, failures, and outages. Updates and maintain operational system documentation and standard operating procedures.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering, accounting or business administration or a related field. Five (5) years directly related experience in high performance computing field may be substituted for the educational requirement.

Experience:

Technical knowledge of LAN/MAN/WAN operations and UNIX environments is required. Five (5) years hands-on experience as a UNIX LAN Administrator is required, and technical knowledge of high performance computing operations is desired. It requires previous experience and ability in providing

technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

4 INFRASTRUCTURE DEVELOPMENT AND IMPLEMENTATION SERVICES

IT Infrastructure Development and Implementation Services provide for the **development, integration, and implementation** of all information technology infrastructure resources including desktop systems, local and wide area network systems, high performance desktop and network systems, telecommunications, video-telecommunications, and Data Center, and other related Tier 3 technical support.

4.1 Systems Engineering

Infrastructure Development and Implementation Branch (IDIB) performs as an overall NRC IT infrastructure architectural engineer, providing strategic recommendations, planning, coordination, design, development, testing, and integration for all NRC IT infrastructure projects, systems, applications, and future requirements.

4.1.1 IT Infrastructure Development

IDIB develops a comprehensive IT Infrastructure architectural strategy to meet the changing mission requirements of the NRC and to maintain compliance with service level requirements. IDIB develops the short and long range plans necessary to implement the strategy. IDIB provides specific system requirements for additions, changes, upgrades and deletions to the applications and equipment necessary to implement the strategy.

4.1.2 IT Infrastructure Integration

IDIB provides all technical services needed to integrate changes to the applications and equipment of the NRC IT Infrastructure Production Operations Environment (POE). The life-cycle of required developmental/integration activities includes, but is not limited to development and/or refinement of functional requirements; analysis of alternative conceptual designs; test and evaluation of pilot systems; demonstration of new capabilities to NRC end-users; integration of new capabilities with existing network hardware and software products; development of implementation plans including costs estimates, scheduled rollout, resources required, etc.; training of contractor personnel; training of NRC staff (but not end users); training plans for NRC end users; and operational cut-over plans.

Examples of development and integration projects include, but are not limited to:

- Workstation application or equipment upgrades or changes
- Revision of Workstation images
- New Workstation scripts
- New NT upgrades
- Network server application or equipment upgrades or changes
- Unix workstation or server application or equipment upgrades or changes
- New firewall appliances, proxy servers, and caching devices

4.1.3 IT Infrastructure Implementation

IDIB provides testing, network performance impact analysis, network modeling and simulation, integration, demonstration, product briefings, evaluation, and orientation/training. As part of this activity, comparison of alternative solutions and determination of the most cost-effective configurations and implementation

alternatives to meet end-user needs is performed.

4.2 IT Infrastructure Services

4.2.1 Workstation System Services

IDIB provides life cycle development and integration services for the NRC workstation image which is deployed Agency-wide on all NRC workstations. Elements to be supported include the operating system, standard office automation applications such as E-mail, scheduler/calendar, word processor, spreadsheet, presentation graphics, web browser, the upgrade to a new office automation suite, support for multi-media, network connectivity, local and network printers, drivers, and utilities etc. Also included is a requirement to support the development and upgrade of workstation and peer server/workstation configurations at the NRC's resident inspector sites, special remote computing workstations, laptop systems and docking stations.

4.2.2 Local and Wide Area System Services

4.2.2.1 Infrastructure Services

IDIB provides life cycle development and integration services for all development efforts related to NRC Local and Wide Area Network projects. Elements to be supported include Network hubs, switches and routers; Internet connectivity; WAN connectivity to remote locations (regions, resident inspector sites, LABS, NIH, etc.), remote/dial-up access; video teleconferencing; video streaming; video consolidation, Virtual Private Networks (VPNs), and audio telecommunications systems. Also included is (1) development of related hardware and software, and (2) a capability to manage connectivity and monitor services used on each infrastructure device circuit or virtual circuit.

4.2.2.2 Web Architecture Services

IDIB supports the Web Architecture environment at the NRC. Elements supported include Unix and NT servers, Netscape/iPlanet and IIS Web servers, Tuxedo and ColdFusion application environments, LDAP compliant directory, and Sybase and SQL/Server DBMS. IDIB develops and implements the web site infrastructure to support end-user development, configuration of the web server to enable Secure Sockets Layer, establishes a three-tier architecture using ColdFusion in the middle tier, develops application server platforms to include a Web Publisher platform including publishing rules, engineers a framework for utilizing LDAP-compliant directory with a three-tier security implementation, and creates a distributed content management framework to support end-user development with authoring tools available for use by program offices.

4.2.2.3 LAN/WAN Server Services

IDIB provides life cycle development and integration services for all IT Infrastructure file, application, remote computing, printer, Web and other servers. Support required includes responsibility for development and enhancements of all component parts of the physical hardware platform, storage systems and media, operating systems, backup systems, CD storage systems, UPS's, groupware, client drivers, NDS and server management utilities, and any other ancillary devices and applications associated with these servers.

4.2.3 High Performance Computing Environment (HPCE) Services

IDIB provides HPCE workstation and server systems life-cycle development and integration services. Elements supported include the applications (unique, or vendor supplied scientific code), operating systems, physical hardware platforms, storage systems and media, the backup systems, CD storage systems, network printers, UPS's, client drivers, server management utilities, and any other ancillary devices and applications associated with these workstations and servers. IDIB is responsible for assisting nuclear engineers with troubleshooting scientific code integration issues if they do not run properly within the NRC environment. The servers are primarily located in three separate rooms that support the Program Offices and consist of mostly Unix servers and workstations. IDIB is responsible for coordinating server installation and repair as needed with vendors under the terms of purchase or hardware/software support contracts. Duties include configuration of COTS software, management of license key generators, support for printer and plotter driver integration and analysis and management of memory performance based on statistics. Support also includes mail routing troubleshooting, database migration efforts, management of tape backup scripts and running of special tape backups, modification of directory structures, and assisting users with file transfer protocol problems as well as the installation of SQR, COBOL, C, and other languages and compilers as required.

4.2.4 Other IT Infrastructure Services

4.2.4.1 IT Infrastructure Security Services

IDIB provides life cycle development and integration services for IT infrastructure and workstation security. This includes providing protection from both external and internal sources and allows a working balance of available services and reliable security. Support required includes responsibility for development and enhancements of all component parts of Internet firewalls, e-mail systems, intrusion detection systems, web servers, network management systems, Dynamic Host Configuration Protocol (DHCP) capabilities, audit trail and alert capabilities, Electronic Commerce, Electronic Information Exchange, public access, virus protection, digital certificates, digital signature capabilities, and the monitoring of Computer Emergency Response Team (CERT), Computer Incident Advisory Capability (CIAC), and European Organization for Nuclear Research (CERN) security bulletins, as well as the daily review of firewall, and Intrusion Detection System (IDS) logs using appropriate scripts and native operating system commands in search of anomalies and responding to them and notifying the NRC. IDIB reviews and analyzes the logs and prepares a monthly report on Internet intrusion attempts. IDIB responds to hacker break-ins, assists with the conduct of independent security audits, analyzes security filtering/functionality problems, responds to security threats like the Berkeley Internet Name Domain (BIND) vulnerability, and tests and maintains Sendmail and IDS RealSecure software at current versions.

4.2.4.2 Contingency Management

IDIB develops/reviews and updates if necessary, the contingency management plans to support the NRC IT Infrastructure in the event of a loss of primary or critical IT infrastructure services; designs, plans, and implements as necessary, the components required to support the NRC IT infrastructure in the event of a loss of primary or critical IT infrastructure services; provides support in performing recovery operations in the event of a catastrophic network failure, loss of critical network elements, and/or for purposes of testing of the contingency systems/plans; performs semiannual audits of compliance with NRC disaster recovery procedures; responds to reports generated from independent audits of procedure compliance; and supports disaster recovery site (s) to ensure viability of recovery at remote sites in the event of a HQ disaster.

4.2.4.3 Procurement

IDIB procures services, support, hardware and software for NRC prototype and production systems to support the design, development, integration, and implementation of NRC applications or equipment. Procured products include, but are not limited to: desktops, laptops, printers, and network components such as: servers, hubs, routers and other auxiliary components connected to the network.

4.3 Development, Integration, and Implementation Life-Cycle

The NRC has implemented the Infrastructure Development Process Model (IDPM) as the standard life-cycle methodology for release management of new technology to the Production Operation Environment (POE), or modifying existing systems within the POE. In introducing NRC applications into the NRC POE, the "Development Process Model (DPM)" is followed. It ensures that the development and/or integration tasks 1) result in effective design, testing, and integration of applications that pass production testing, 2) are integrated into production without adverse impact on the POE, and 3) perform as designed. The number and scope of DPM activities vary from project-to-project based on the degree of complexity.

All development/integration projects generally include the stages described below.

4.3.1 Detailed Requirements Analysis

- Analyze new NRC requirements, industry trends, and technology advances related to NRC network and workstation infrastructure.
- Provide requirements analyses, needs assessments, recommendations and business cases for system upgrades, design modifications, and additional capabilities.
- Meet with NRC users and technical staff to define the users' requirements.
- Determine impact of new development on production environment.
- Make a determination of project feasibility.

4.3.2 Design

- Develop conceptual and detailed system designs.
- Identify the technical teams involved in design and development.
- Create detailed functional specifications.
- Prepare a detailed conceptual design.
- Obtain approval of the functional specifications and conceptual design by the NRC.
- Prepare one or more technical designs.
- Prepare an integration plan, with product specifications, project schedule, resource requirements,

budget estimates, and option comparisons.

- Conduct a technical review.

4.3.3 New Technology Development

- Develop new systems, system upgrades, and automated upgrade processes based on the technical designs.
- Purchase, assemble, and/or build the components and systems.
- Perform custom integration as required.
- Make changes to the technical design, as needed.
- Develop the tools needed to be added or modified in the Integrated Network Management System (INMS) to provide management and automated monitoring of the new technology and to provide the data required for reporting.
- Prepare a user guide and any changes required of the detailed design document and technical specifications.
- Prepare the support, operations and maintenance plan for the new technology.
- Prepare and obtain approval of a comprehensive test plan based on the functional specifications.

4.3.4 New Technology Acceptance Testing

- Conduct a stakeholders review of the Acceptance Test Plan.
- Operate a network test laboratory and staging facility to support network related testing, network performance analysis, modeling and simulation and staff orientation.
- Conduct internal testing, in an isolated controlled environment (test lab).
- Develop conceptual and detailed plans for testing and evaluation of pilot IT infrastructure capabilities, and to demonstrate new capabilities.
- Conduct progression/regression testing to ensure that new IT infrastructure products or systems do not adversely affect the existing and future production operations environments.
- Coordinate testing with applications support personnel.
- Perform user tests to assure that the systems/upgrades will meet the needs of NRC staff per the original analysis.
- Conduct load and stress, functionality, and other tests as defined in the Acceptance Test Plan.

- Document and publish test results.

4.3.5 Transition to Production Operational Support

- Complete any outstanding documentation, and any outstanding final approvals.
- Develop and execute operational cut over plans.
- Train the NOC and CSC staff members in installation and support of the new technology.
- Integrate lessons learned into documentation and product, with NOC and CSC staff participation in finalizing any document or new technology changes.
- Obtain approval of the final implementation schedule.
- Purchase the necessary hardware and/or software licenses required for Agency-wide rollout.

4.3.6 Implementation

- Work with Network Operations Center and Customer Support Center to implement new products.
- Provide on-call telephone and on-site assistance to the NOC and Customer Services Center during implementation and as a secondary level of operational support.
- Provide support for restoration of prior configurations if necessary to maintain operational integrity.

3.7 Position Descriptions

Beginning on the following page and continuing through the remainder of the section are the position descriptions the Contractor is required to fill. Not all positions must be filled at all times. All key positions shall be filled at the initiation of activities under this contract. In addition, certain additional positions shall be directed by the NRC to be filled. Other positions (e.g., consultants) shall be filled only during certain times and with the direction of the NRC. The position descriptions are a catalog of skills the Contractor will be required to provide.

4.3.7.1 LAN Administrator

POSITION DESCRIPTION

Position: LAN Administrator

Functions: Provide user specific support such as troubleshooting and solving software problems, and determining hardware problems (e.g., Printing, NIC cards, WordPerfect). Operates, monitors, and administers servers, workstations and printers, associated peripheral equipment, and network environment. Maintains scheduled reports of LAN/WAN operations activities. Recognizes problems and requests assistance. Administrates system user accounts.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science or a related field. Five (5) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

Four (4) years experience as a Novell or NT LAN Administrator is required, and technical knowledge of UNIX LAN operations is desired. This position requires a sound knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet various NRC requirements. It also requires the ability to deal effectively with NRC personnel.

4.3.7.2 LAN Systems Analyst

POSITION DESCRIPTION

Position: LAN Systems Analyst

Functions: Provides Novell and/or Windows expertise.

Performs activities associated with design and implementation of local area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local area network, office automation and microcomputer systems applications. Performs comparative analyses of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training guidance for the NRC. Assists local area network analysts and programmers with planning, organizing, controlling, and scheduling of activities.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering, statistics, operations research, accounting or business administration. Five (5) years directly related experience in the networking field may be substituted for the educational requirement. If the position is for a Novell product, the individual shall be a Certified Novell Engineer (CNE) or have equivalent on-the-job experience. If the position is for a Microsoft product, the individual shall be a Microsoft Certified Systems Engineer (MCSE) or have equivalent on-the-job experience.

Experience:

At least five (5) years of experience with progressively more difficult LAN/network responsibility and with a minimum of three (3) years of systems analysis, to include work as an analyst for complex office automation and local area network systems. This position requires a sound, thorough, practical and theoretical knowledge of local area networks and office automation systems. It requires previous experience and ability in providing technically sound hardware and/or software solutions to meet current and expanding Novell and/or NT and network requirements. It also requires initiative, imagination, analytical ability, and the ability to deal effectively with NRC personnel.

4.3.7.3 Network Analyst

POSITION DESCRIPTION

Position: Network Analyst

Functions: Major participant in all network discussions ranging from problem definition through problem solution of major projects. Works with minimum supervision. Prepares substantial parts of interim and final reports. Often assigned more than one task at a time, and therefore, must be capable of effectively planning the use of time and must be able to divide time among several tasks. Generally has extensive contact with NRC staff. Generally designated as project leader of a small to medium sized project or a portion of a larger one. Performs services as a technical expert in one or more of the following areas:

Local and wide area network planning, design, testing, integration and engineering.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in telecommunications, electrical engineering, computer science or related fields. Six (6) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

At least five (5) years of experience with progressively more difficult LAN/network responsibility in design of wide area network, office automation and network systems is required. This includes 2 years in design of wide area networks, and office automation systems, telecommunications systems and 1 year in network management. This position requires good analytical and problem solving ability, creativity and insight. Requires skills in verbal and written communications.

4.3.7.4 Security Analyst

POSITION DESCRIPTION

Position: Security Analyst

Functions: Performs activities associated with the implementation and support of security systems on the Local and Wide Area Network services in Novell, NT and UNIX environments, and between that network and the Internet. Evaluates, installs, customizes and integrates commercial and custom security applications and hardware. Programs specialized applications as necessary to meet security requirements.

Implements and maintains security "firewalls" between networks, especially between NRC networks and the Internet.

Conducts user and technical training, and provides guidance in the operation and use of security applications throughout the NRC environment.

Provides trouble shooting and problem resolution for Novell, NT and UNIX security applications.

Assists other staff and programmers in the security aspects of design, development and implementation. May act as project manager.

Maintains liaison with the security community in order to obtain the most current security advisories and otherwise remain current on security matters and to keep the NRC security system current.

Performs the analysis and design of automated systems/subsystems requirements with particular emphasis on security matters such as encryption, verification and authentication. Develops programs, C-shell scripts, and other work for the implementation of security systems for network applications.

Qualifications:

Education:

Bachelors level degree from an accredited university or college in computer science, mathematics, engineering, accounting or business administration is required. Six (6) years directly related experience as a security programmer of which at least two years were as a security analyst may be substituted for the educational requirement.

Experience:

Minimum five (5) years of ADP experience, preferably three years programming experience and two year experience in problem analysis and/or system design. This position requires a minimum of two (2) full years of sound, thorough, theoretical and practical knowledge of security systems and related programming gained through experience. Specific experience is desirable with network security (UNIX security experience mandatory), firewalls, Internet security and network protocols. This position requires previous experience and ability in providing technically sound hardware and/or software security solutions to meet current and expanding network requirements. Position also requires initiative, imagination, analytical ability and the ability to deal effectively with NRC personnel. Previous work with federal government agencies is desirable.

4.3.7.5 Senior Systems Architect/Engineer

POSITION DESCRIPTION

Position: Senior Systems Architect/Engineer

Functions: Provides technical support to the NRC long range plans for network upgrades and enhancements. Works with users and staff to develop requirements and to analyze and recommend alternative approaches to meet those requirements.

Performs activities associated with the design and implementation of local and wide area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local and wide area networks, office automation systems and microcomputer systems and applications. Performs comparative analysis of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training. Assists LAN Analysts and programmers in the planning, organizing, controlling and scheduling of activities. May act as project manager.

Serves as the technical expert in the area of measurement and analysis of LAN, WAN, and OFFICE AUTOMATION systems hardware and software. Measures and reports on the performance of LAN, OFFICE AUTOMATION, ADP, and telecommunications systems. Maintains the performance database,

performs performance analysis to identify and seek solutions to performance problems.

Provides administrative and technical consultation on a wide variety of management concerns such as: office and automation studies, system and processing problem areas, areas for potential improvement, and methods and procedures to promote the efficiency and effectiveness of office systems operations. Provides guidance and management analysis capabilities to resolve processing and office system operation problems.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, electronics, mathematics, engineering, statistics, operations research, accounting, business administration, or computer related field is desirable. Ten (10) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

At least ten (10) years experience with progressively more difficult LAN/network responsibility including a minimum of eight (8) years of systems analysis including acting as lead analyst for development of LAN, WAN and OFFICE AUTOMATION systems. This position requires a sound and thorough theoretical and practical knowledge of LAN, WAN and office automation systems. Requires skills in verbal and written communications. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with customers and NRC network staff. Previous work with federal government agencies is desirable.

4.3.7.6 Senior Systems Consultant

POSITION DESCRIPTION

Title: Senior System Consultant

Functions: Serves as senior technical advisor on complex projects as determined by the Contractor or requested by the NRC. May serve as team leader on difficult or significant projects. Provides technical expertise when assigned to a project. May be required to participate in any phase of major project from concept definition through implementation and support. May be assigned to several concurrent tasks. Will have close contact with customers at all levels of the NRC. Provides expertise in the following areas:

1. Integration of LAN/MAN/WAN and Office Automation Systems,
2. Design of multi-vendor LANs interconnected via multiple protocols,
3. Evaluation of LAN/MAN/WAN, and OFFICE AUTOMATION Systems software and hardware,
4. Evaluation, development, planning, installation, operation, maintenance of multi-vendor LAN systems including technologies such as 10/100/1000/10000 Ethernet, Novell, NT, UNIX, TCP/IP, IPX, Corel WordPerfect Office, Novell GroupWise, and the Internet.
5. Any other network related area of expertise as directed by the NRC.

Qualifications:

Education:

Masters level degree from an accredited university or college is required in electrical engineering,

management science, computer science, mathematics, industrial, or other engineering discipline. Fifteen years experience in network technology in general and three years in the requested speciality may be substituted for the educational requirement. Five (5) years experience in network technology and one year in the requested speciality combined with as BS or BA in the delineated fields may be substituted for the educational requirement.

Experience:

At least eight (8) years of technical related experience is desirable, including two (2) years in program/project management. To be effective the individual should have demonstrated analytical and problem solving ability, creativity, and insight in working with networks similar to the NRC's. In addition the individual should have strong verbal and written communication skills.

Special Note:

This position may be a full time position with the Contractor if the NRC agrees that such skills are required on the contract. However, the job description may also be used by the NRC and the Contractor as a method to obtain temporary consulting services in areas of expertise outside that of the Contractor's normal staff.

4.3.7.7 Senior Systems Engineer

POSITION DESCRIPTION

Position: Senior Systems Engineer

Functions: Performs activities associated with the design and implementation of local and wide area networks and office automation systems. Analyzes, designs, integrates documents, implements "state of the art" local and wide area networks, office automation systems and microcomputer systems and applications. Performs comparative analysis of commercial software packages. Conducts scientific and statistical analyses. Conducts user and technical training. Assists LAN Analysts and programmers in the planning, organizing, controlling and scheduling of activities.

Serves as the technical expert in the area of measurement and analysis of LAN, WAN, and OFFICE AUTOMATION systems hardware and software. Measures and reports on the performance of LAN, OFFICE AUTOMATION, ADP, and telecommunications systems. Maintains the performance database, performs performance analysis to identify and seek solutions to performance problems.

Provides administrative and technical consultation on a wide variety of management concerns such as: office and automation studies, system and processing problem areas, areas for potential improvement, and methods and procedures to promote the efficiency and effectiveness of office systems operations. Provides guidance and management analysis capabilities to resolve processing and office system operation problems.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, electronics, mathematics, engineering, statistics, operations research, accounting, business administration, or computer related field is desirable. Ten (10) years directly related experience in the networking field may be substituted for the educational requirement.

Experience:

At least eight (8) years experience with progressively more difficult LAN/network responsibility including a minimum of seven (7) years of systems analysis including acting as lead analyst for development of LAN, WAN and OFFICE AUTOMATION systems. This position requires a sound and thorough theoretical and practical knowledge of LAN, WAN and office automation systems. Requires skills in verbal and written communications. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with customers and NRC network staff.

4.3.7.8 Systems Consultant

POSITION DESCRIPTION

Title: Systems Consultant

Functions: Major participant in any project or phase of development from problem definition through problem resolution. Works with minimum direct supervision. Responsible for preparing substantial parts of interim and final reports. Can be expected to work on multiple tasks simultaneously and must be able to effectively plan and manage own time. Will have extensive contact with NRC staff as requested by the NRC. Can serve as project manager of small or medium sized projects or portions of larger ones. Will provide expertise in the following areas:

1. Local and Wide Area Networks and office automation Systems,
2. Resource sharing capabilities,
3. Evaluation of LAN, WAN, and office automation systems software and hardware,
4. Development, maintenance, planning, engineering, and management of telecommunications (data communications, communications security, and networking) systems,
5. Development, planning, evaluation and review of LAN, WAN and office automation systems security.
6. Any other network related area of expertise as directed by the NRC.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in management sciences, computer science, mathematics, industrial or other engineering, accounting, or business administration. Ten (10) years experience in network technology in general and one year in the requested speciality may be substituted for the educational requirement.

Experience:

At least 5 years of related experience is required, to include 2 years in professional consulting and 1 year in project management. This position requires proven analytical and problem solving abilities, creativity and insight. Skill in making verbal and written presentations is required.

Special Note:

This position may be a full time position with the Contractor if the NRC agrees that such skills are required on the contract. However, the job description may also be used by the NRC and the Contractor as a method to obtain temporary consulting services in areas of expertise outside that of the Contractor's normal staff

4.3.7.9 UNIX System Analyst

POSITION DESCRIPTION

Position: UNIX System Analyst

Functions: Performs activities associated with the implementation and support of UNIX Systems, and the development and implementation of Local and Wide Area Network services in a UNIX environment. Evaluates, installs, and integrates commercial UNIX software packages. Conducts user and technical training, and provides guidance in the operation of NRC UNIX Workstations and network environments. Provides trouble shooting and problem resolution related to UNIX network environment. Assists LAN Analysts and programmers in the design and development of Novell and UNIX interconnected networks and connectivity. May act as project manager.

Qualifications:

Education:

Bachelors level degree from an accredited university or college is required in computer science, mathematics, engineering statistics, operations, accounting or business administration. Five (5) years directly related experience as a UNIX analyst of which at least two (2) years as a UNIX systems administrator may be substituted for the educational requirement.

Experience:

At least three (3) years experience including two (2) years experience in the UNIX environment. This position requires a sound, thorough, theoretical, and practical knowledge of UNIX, LAN and Office Automation systems. It also requires initiative, imagination, analytical ability, and the ability to deal tactfully and effectively with NRC personnel.

5 PROGRAM SERVICES

Program Services provides continuity and control of specific functions that affect all of the ITID Branches.

These functions include:

- Quality Management
- Configuration Management
- Contingency Management
- Documentation Management
- Security Management
- Independent Audit and Verification

For each of these functions Program Services has developed a program that is used throughout the ITID Organization by all contractors. Program Services also assists individual Branches and contractors in developing plans, automated systems, metrics, methods for analysis, reporting and other requirements necessary to conform to the program objectives.

5.1 Quality Management

5.1.1 Program Management

- Develop and maintain a Quality Management Program for all services performed.
- Update the plan semi-annually.

5.1.2 Metrics and Performance Criteria

- Assist in developing metrics and performance criteria to determine whether or not established service levels are being met in carrying out their mission.
- Maintain and electronically store performance data derived from automated systems supporting services provided.

5.1.3 End-User Satisfaction Monitoring

- Conduct periodic, statistically significant, random surveys to assess end-user satisfaction with services provided.
- Produce an end-user satisfaction report based on the results of the end-user satisfaction survey.
- Develop and implement procedures to continue to meet service goals.

5.1.4 Trend Analysis

- Develop trend analyses to ensure early identification of areas requiring special attention.
- Perform Trend Analysis as needed.
- Collect Service Request resolution data.
- Monitor hardware problem records for each IT component.
- Monitor software problem records for each IT component.
- Track and report by office, the number of tickets that are simply questions about the use of systems (training requests).
- Recommend changes or solutions to NRC on the following:

- Problem areas.
- Information that will assist application training in the NRC Professional Development Center.
- Changes to the NRC infrastructure that are problematic.
- Changes in the way development introduces new upgrades to NRC Agency-wide applications, based on how it impacts support and the level of increased effort.
- Monitor and discuss with NRC the observation and record of similar, identical, or repetitive CSC Service Requests, especially those that emanate from one particular office, client, building/floor, or office designation.
- Participate in information gathering or technical problem studies as requested by NRC.

5.1.5 Reporting

- Report monthly on actual performance results as compared to the performance goals.
- Provide weekly and quarterly trend analysis reports.
- Provide CSC Service Request summaries.

5.1.6 OCIO Coordination

- Participate and assist in the integration of services support into all planned upgrades, enhancements, and updates to the NRC infrastructure prior to roll-out.
- Attend meetings to assist in the development and implementation of plans for proposed changes in the operation of applications.

5.1.7 Audits

- Assist in responding to NRC reports generated from independent audits of procedure compliance.

5.2 Configuration Management

5.2.1 Program Management

- Develop and maintain a Configuration Management Program
- Assist in the development of configuration management components specific to other OCIO Groups that will integrate with the ITID Configuration Management Program.

5.2.2 Change Management

- Assist in developing and monitoring procedures for reporting, verifying, and recording all changes made to hardware, software, firmware, and documentation throughout the system's life cycle.

5.2.3 Hardware/Software Inventory

- Develop, implement, and maintain an Inventory Management Program to track the physical equipment within NRC.
 - Assist in developing inventory components specific that will integrate with the ITID Inventory

Management Program.

- Participate in and support the annual inventory of NRC property.
- Provide Property and Supply System (PASS) updates.

5.2.4 Configuration Management Data Base (CMDB)

- Develop and implement a plan for identifying, defining and registering CMDB configuration items.
- Select supporting tools
- Register configuration items.
- Establish the current CMDB baseline.
- Maintain updated information on current systems.

5.2.5 Configuration Reporting

- Provide configuration reports as required.
- Maintain and provide infrastructure maps and logic diagrams as required.

5.3 Contingency Management

5.3.1 Program Management

- Develop and maintain an ITID Contingency Management Program
- Assist in the development of contingency management components specific to other OCIO Groups that will integrate with the ITID Contingency Management Program.

5.3.2 Backup

- Develop and monitor backup policies and procedures to ensure the ability to recover and restore NRC systems, applications, files and data.
- Assist in developing backup schedules for all systems and data.
- Assist in creating back-up copies of system hard drives in compliance with standard operating procedures.
- Assist in validating the integrity of back-up copies.
- Assist in providing for data and system software restoration
- Perform semiannual audits of compliance with backup policies and procedures and report the audit findings to NRC.

5.3.3 Disaster Recovery

- Develop a disaster recovery plan in the event of a catastrophic network failure and/or loss of critical network elements.
- Support a disaster recovery site to ensure viability of recovery at remote sites in the event of NRC headquarters disaster.
- Execute the disaster recovery plan in the event of a catastrophic network failure and/or loss of critical

network elements.

- Assist other OCIO groups in developing individual disaster recovery plans that integrate with the ITID disaster recovery plan.
- Respond identified network disasters as required by the disaster plan and in accordance with NRC policies, procedures and service level requirements.

5.4 Documentation Management

5.4.1 Program Management

- Develop and maintain an ITID Documentation Management Program for use by all services provided to assure the comprehensive, detailed, up-to-date documentation of NRC policies, processes, procedures, systems, applications, and other documentation required for the ongoing maintenance of ITID activities.
- Assist in the development of documentation management components specific to other OCIO Groups that will integrate with the ITID Documentation Management Program.

5.4.2 Procedures

- Develop, document (in a easy-to-access and search manner), and maintain standard operating procedures for all Desktop Systems activities.
- Continually review and comment on Desktop Systems standard operating procedures to improve efficiency, improve user support, reduce cost, or otherwise improve operations of Desktop Systems.
- Provide Standard Operating Procedures to OCIO Project Officer and OCIO staff, as requested.
- Update and modify processes and procedures within 30 days of any significant change.
- Provide assistance implementing OCIO policies and procedures as they pertain to Desktop Systems support issues.
- Respond to NRC independent audits of procedure compliance.

5.5 Security Management

5.5.1 Program Management

- Develop and maintain an ITID Security Management Program for use by all OCIO Groups.
- Be familiar and comply with existing NRC security policies and plans and maintain cognizance of procedures and standards promulgated by the National Institute of Science and Technology (NIST) as well as the commercial environment.
- Assist in the development of security management components specific to other OCIO Groups that will integrate with the ITID Security Management Program.

5.5.2 System

- Identify and develop requirements and implement security measures to ensure appropriate safeguards are in place for all system components and services.
- Assist each OCIO group to:
 - Identify, evaluate, develop, implement and operate automated tools to monitor and manage security.
 - Develop and maintain systems that automatically examine logs for unauthorized access attempts or

- suspicious activities.
- Take necessary action to prevent and stop unauthorized access and/or suspicious activity.
- Gather and analyze statistical security information and provide recommendations to improve and enhance security.
- Implement data security, file conversion, and file and data backup policies.
- Control access to administrator rights and passwords.
- Ensure all systems have and use security capabilities meeting NRC's minimum standards.
- Provide End-User ID administration.
 - Develop, document, and follow step-by-step account administration processes and procedures for every scenario to assure the continuity of support staff performance.
 - Update the account administration processes and procedures as necessary to conform with current operations.
 - Provide OCIO staff (as identified by the Project Officer) a copy of the account administration processes and procedures.
 - Provide password administration (including resets, automatic expirations).
 - Provide end-user account management.
 - Provide account security precautions.
 - Provide shared file access management and administration.
 - Administer access control lists for directory, library, and categories.
 - Set up system defaults for user and group profiles.
 - Set up default access rights for users and groups.
 - Set up and administer the Administrator group, including adding and deleting users.
 - Maintain user profiles.
 - Support, revise, and implement standards for assignment of privileges.
 - Provide security capabilities for all CSC systems in accordance with NRC policies and procedures.

5.3 Network/Cyber

- Identify and develop requirements and implement security measures to ensure appropriate safeguards are in place for network components, systems and services.
- Identify, evaluate, develop, implement and operate automated tools to monitor and manage network security.
- Develop and maintain systems that automatically examine network access logs for unauthorized access attempts or suspicious activities.
- Take necessary action to prevent and stop unauthorized network access and/or suspicious activity.
- Evaluate, develop, implement and continuously update virus protection software as required for network and desktop components, systems and services.
- Gather and analyze network and desktop statistical security information and provide recommendations to improve and enhance network security.
- Provide recommendations and maintain adequate physical security measures for network components and systems.
- Perform periodic audits to ensure compliance with security procedures and processes and report results to NRC.
- Implement data security, file conversion, and file and data backup policies.
- Provide operational maintenance, upgrade, and support of the NRC Firewall components and systems.

5.5.4 Physical

- Provide recommendations and maintain adequate physical security measures for network components and systems.
- Assist each OCIO group to restrict physical access to rooms with critical systems.
- Assist each OCIO group to control access to facilities where sensitive NRC data may be at risk.

5.5.5 Audits

- Assist each OCIO group to respond to NRC independent audits of compliance with CSC security policies and procedures.

5.6 Independent Audit and Verification

- Perform semiannual audits of compliance with NRC policies and procedures for:
 - Configuration Management
 - Backup
 - Disaster Recovery
 - Documentation
 - Security
- Report the audit findings to NRC.
- Report the findings to other contractors.

6 RELATED NRC IT SERVICES

The following NRC IT services are not covered under this SOW. They are briefly discussed here for information only.

6.1 TELECOMMUNICATIONS SERVICES

Telecommunications Services provides voice services at the NRC's headquarters location. The NRC participates in GSA's Washington Interagency Telecommunications System (WITS) and FTS2000/FTS2001 programs that provide for local and long distance telephone service to Federal customers in the Washington area.

Telecommunications Services also provide and manage the additional telecommunications contracts that furnish additional services not included in the Governmentwide contracts. The systems and equipment supported include, but are not limited to, CENTREX, ISDN, PBX systems, key systems, facsimiles, pagers, cellular phones, satellite communications, two-way radios, audio and video conferencing systems, and cable TV services. The cable plant operation, support and maintenance is included in this grouping based on budgetary categorization.

Telecommunications Services provide the NRC message center and switchboard, telephone and video conferencing, voice mail, calling cards, pagers, facsimile machines, modems, cellular telephones, wire services, secure communications, telex messages, telecommunications devices for the deaf (TDD), and Emergency Operations Center communications.

2 DATA CENTER SERVICES

The Data Center provides system environments for Agencywide applications, including equipment, administration, operation, and support.

The Data Center provides security, operations, support, and maintenance of all mini and mainframe computer systems.

The following applications are provided through the NRC Data Center and are available for use from any Agencywide desktop system when the appropriate access software is installed. These services are provided 24 hours a day, five days a week, with additional on call support provided as required.

ADAMS	Voter Tracking System
Payroll	Commissioner's Calendar
Personnel	EXSIS
Property	GLDB
Criminal History	SIMS
Thesaurus	LMS
STARFIRE	Emergency Response Data System (ERDS)
	Allegation Management System (AMS)
	Executive Shared Information System (EXSIS)

The following applications are provided through a timesharing service. The applications are available from

Agencywide desktop systems when special Agencywide software is installed and a valid user account is issued.

Regulatory Information Tracking System
Agency Training System
Automated Personnel System
Annual Material License Fee

Operator Licensing Tracking System
Manpower System
Technical Assignment Control System

The following applications will be provided through a timesharing service until STARFIRE (the NRC administration services program) is fully implemented and supported.

Federal Financial Management System (FMS) (120 accounts)
NRC's Financial and Accounting Applications (120 accounts)
Payroll/Personnel System (1,076 accounts)
Production Time and Attendance Data Entry (1,076)

6.3 EMERGENCY OPERATIONS CENTER

OCIO provides operation and maintenance support to the IT Infrastructure components located in the NRC Emergency Operations Center on the 6th floor of Two White Flint North. Some SMS support will be required each time the Center is fully activated.

NRC's Emergency Operations Center is intended to ensure the continued, uninterrupted exchange of information between HQ and any incident site involving nuclear materials, including the four Regional Offices, Nuclear Power Plants, fuel and waste sites, and other governmental agencies.

Within the Washington, D.C. metropolitan area, NRC uses Verizon, FTS 2001, GSA Consolidated Local services, and WITS, as well as sharing services with the Department of the Interior's National Interagency Fire Center.

In addition to the refresh, maintenance and support of desktops, servers and peripherals, ITID is responsible for performing the following tasks for the Emergency Operations Center:

- 1) Provide the facilities, services, and equipment required to support both wire, and wireless voice, data and video communications.
- 2) Provide Emergency Telecommunications Specialist Coordination support.
- 3) Update and distribute current copies of the PBX system charts.
- 4) Maintain the Emergency Telecommunications Response Workbook.
- 5) Provide operation and maintenance of the PBX system and associated telecom equipment and services.

PERSONAL RECORD CONSIDERATION CHECKLIST

Use the checklist below to assist you in making a determination as to whether your records are personal or agency records. If you have any questions, contact your office FOIA coordinator or OCIO/FOIA staff.

	YES	NO
Creation - Was the document created by an agency employee on agency time, with agency materials, at agency expense? (If not, then it very likely is not an "agency record," on that basis alone.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Content - Does the document contain "substantive" information? (If not, then it very likely is not an "agency record," on that basis alone.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
---	-------------------------------------	--------------------------

Does it contain personal as well as official business information?	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------

Purpose - Was the document created solely for an individual employee's personal convenience? Alternatively, to what extent was it created to facilitate agency business?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
---	--------------------------	-------------------------------------

Distribution - Was the document distributed to anyone else for any reason, such as for a business purpose? How wide was the circulation?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
---	-------------------------------------	--------------------------

Use - Did the document's author actually use it to conduct agency business (i.e., prepare an agency document)? If yes, to what extent did others use it?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
---	-------------------------------------	--------------------------

Maintenance - Was the document kept in the author's possession? Was it placed in an official agency file?	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
---	--	--

Disposition - Was the document's author free to dispose of it at his personal discretion? What was the actual disposal practice?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
---	--------------------------	-------------------------------------

Control - Has the agency attempted to exercise "institutional control" over the document through applicable maintenance or disposition regulations? Did it do so by requiring the document to be created in the first place?	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
---	--	--

Segregation - Is there any practical way to segregate out any personal information in the document from official business information?

Revision - Was the document revised or updated after the fact for record keeping purposes?

I, _____, consider the document(s) in the enclosed envelope, which consists of _____ (number of pages) and pertains to FOIA No. _____, to be "personal records" not agency records.

Author's Signature/Title/Office

Date